# High-Power Microwave Weapons' Effects and Failure Analysis Using Sneak Circuit Modeling

Andrew L. Drozd
ANDRO Computational Solutions, LLC
Rome, New York USA
*adrozd@androcs.com*

Irina Kasperovich
ANDRO Computational Solutions, LLC
Rome, New York USA
*ikasperovich@androcs.com*

***Abstract*— This paper describes a new knowledge-based toolkit approach for analyzing High-Power Microwave (HPM) weapons' effects failure analysis of large, complex systems due to far-field HPM sources as well as close-in High-Power Electromagnetic (HPEM) interferers. In this approach, hybrid frequency/time-domain analytical and numerical techniques are used to assess electromagnetic interference/vulnerability (EMI/V) to HPM fields incident on electronic equipment locations associated with radio frequency (RF) communications systems, electro-optical/infrared (EO/IR) sensors, Global Positioning Systems (GPS), inertial navigation systems (INS), and processors. In particular, failure effects are traced to individual electronic components or devices to quantify HPM weapons' effects failures for front/back-door critical points of entry (POEs) in the system and then component-level HPM failure effects are ranked. The development of new models are described for characterizing HPM EMI/V at the device level, which are not currently available, and that will result in a new expert system capability for performing efficient *sneak circuit fault-tree* type failure modeling and analysis.**

***Keywords*-** *Numerical Models and Modeling, Applications of Coupling to Structures and Cable, System-level Protection and Testing.*

## I. INTRODUCTION

Advanced HPM weapon systems and devices are increasingly being deployed by US adversaries for both defensive and offensive purposes. New emerging threats, proliferation and the success of these mechanisms challenge the EMI/V and survivability of the Navy's current inventory and developmental defense systems, subsystems, and components. Some of these concerns are addressed in MIL-STD-464C. However, the effectiveness of HPM devices is difficult to ascertain because, currently, there is no valid method to determine whether any disruption or damage has occurred especially at the component or device level. Also, there is a need to confidently ascertain the level of damage sustained by enemies in the field from US military HPM weapons.

Since HPM damage may not be readily apparent, a combination of internal signal monitoring and post-test disassembly, investigation, and analysis is often necessary to determine specific failure modes. Limited functional monitoring of the system during testing can make this process extremely problematic and potentially cost prohibitive. Therefore, a need exists to develop a comprehensive analysis methodology and simulation process for understanding as well as quantifying HPM failure effects for various electronics and then prioritizing the effects *vis a vis* severity (temporary disruption, performance degradation, and permanent damage).

More specifically, a capability is needed to more accurately pinpoint potential electronics vulnerabilities, failure modes, as well as the probability and type of failure to incident HPM threats. However, a major challenge is the unavailability of EMI/V data on devices, components and pieceparts and the lack of understanding of HPM-induced failure modes and mechanisms. Hence, there exists a need for developing proven methods of extrapolating or relating susceptibility effects and corresponding EMI/V margins for low-level signal interference in computing HPM DDD thresholds.

Furthermore, HPM coupling and interference/destruction mechanisms are stochastic in nature and thus, have a high degree of variability. HPM devices nominally produce a pulse peak power of $\geq$100 MW and the means of delivery can vary dramatically, such as by an individual, via vehicles, or from large ground structures. Some mechanisms generate a single pulse or multiple pulses creating concerns over victim device non-average power (peak power, energy) vulnerability. Coupling or relating internal signal monitoring methods with damage assessed by inspection is essential to applying techniques for coupling the modeling with the actual HPM effects. Unlike kinetic weapon effects, HPM weapon effects can result in signal-induced EMI/V that in turn, may lead to subtle disturbances or possibly physical damage or even destruction. We can examine and somewhat adapt the processes and assessment methodologies developed in kinetic weapon survivability testing, focusing on electronic forensics and failure analysis, in order to devise a tool that will provide the necessary functionality for assessing incident HPM-induced failure effects.

A potential solution to this problem is to combine a system-level modeling/analysis tool with a statistical electromagnetics (EM) analytical approach in conjunction with an automated "sneak circuit" analysis (SCA) tool consistent with the methodology outlined in MIL-STD-785B tailored to the HPM threat. The SCA approach will provide a computer-based system for the identification of sneak paths and failure concerns in switching circuitry in analog or digital design. The statistical EM and SCA methodology would provide a useful means of classifying HPM coupling modes/mechanisms and effects at the system level for both back-door and front-door (antenna aperture) POEs down to the circuit, device or component level. A *Partial Element Equivalent Circuit (PEEC)* tool has also been considered that can provide a basis for frequency-domain and time-domain EMI/V failure analysis.